A-LEVEL COMPUTER SCIENCE • EXERCISE SHEET

2.1.3 Finding a server: URLs, the Domain Name Service and IP addressing

Name: _____ Class: _____ Date: _____ **Total: 30 marks**

KEY WORDS router 路由器 • ip address IP 地址 • world wide web 万维网 • mac address MAC 地址 • domain name 域名

Objective

Unit 2.1 is large enough to carry three sheets, and between them 2.1, 2.1.1 and 2.1.2 cover the hardware, the topologies, the models and the services. This one takes the two statements none of them reaches, and they are the ones that answer *how a click actually finds a machine*: **how a URL locates a resource and what the Domain Name Service does**, and **how IP addresses are used to transmit data over the internet**. This sheet covers syllabus 2.1.

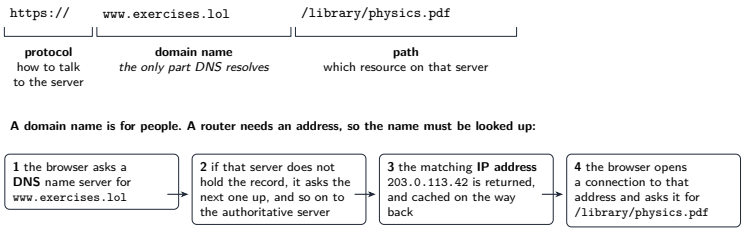
You must be able to:

- explain how a **Uniform Resource Locator** (**URL**) is used to locate a resource on the **World Wide Web** (**WWW**), and the role of the **Domain Name Service** (**DNS**)
- explain the use of **IP addresses** in the transmission of data over the internet, including the format of an IP address (**IPv4** and **IPv6**), the use of **subnetting**, how an IP address is associated with a device, the difference between a **public** and a **private** IP address and the security implications, and the difference between a **static** and a **dynamic** IP address

1 Worked examples

Study these first. Each one shows a **method** that a question later on this sheet needs.

■ A URL has three parts, and DNS only cares about the middle one



Without **DNS** every site would have to be reached by its number, and a site could never change servers without every visitor learning a new address. Caching is what keeps the system usable: the same lookup is not repeated for every page, so the root servers are not asked billions of times a second.

A **Uniform Resource Locator** is the full address of one resource on the **World Wide Web**:

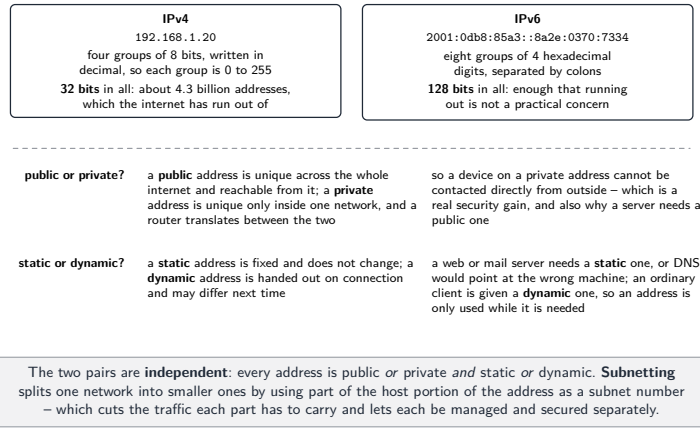
part	example	what it does
protocol	`https://`	which set of rules to talk to the server with
domain name	`www.exercises.lol`	which **server** – the only part DNS resolves
path	`/library/physics.pdf`	which **resource on** that server, handled by the server itself

△ Two careless answers to avoid. The URL does **not** contain the IP address – that is exactly what has to be looked up. And the **path is not sent to DNS**: DNS returns one address for the whole domain, and the server works out which file is wanted afterwards.

The role of the Domain Name Service. DNS is a distributed system of name servers that holds the mapping from **domain name to IP address**. The browser asks a name server for the domain; if that server does not hold the record it passes the query up the hierarchy – root, then the top-level domain, then the **authoritative** server for that domain – until the address is found and returned. Results are **cached** on the way back, in the name servers, the operating system and the browser, so the same name is not looked up again for every page.

Two reasons DNS exists, both worth marks: people can use names that are easy to remember instead of numbers; and a site can be **moved to a different server** by changing one DNS record, with no visitor having to learn a new address.

■ IP addresses: two formats, and two independent pairs of adjectives



- **IPv4 – 32 bits**, written as four denary numbers 0-255 separated by dots (`192.168.1.20`). That is about 4.3 billion addresses, and the internet has run out of them.
- **IPv6 – 128 bits**, written as eight groups of four **hexadecimal** digits separated by colons. It was introduced *because* IPv4 ran out; the vastly larger address space is the reason, not extra speed.
- **How an address is associated with a device**: a device's network interface has a permanent **MAC address** burned in, and an IP address is **assigned** to it on the network – by hand for a static address, or by a **DHCP** server when it connects for a dynamic one. So the IP address belongs to the device's *position in a network*, not to the device.

Public or private. A **public** address is unique across the whole internet and can be reached from it. A **private** address is unique only within one network; a router translates between the private addresses inside and the single public address outside. **Security implication**: a device on a private address cannot be contacted directly from the internet, so it is far less exposed – and, for the same reason, a machine that must accept connections (a web or mail server) needs a public one.

Static or dynamic. A **static** address is fixed. A **dynamic** address is issued when the device connects and may be different next time. A server needs a static address or DNS would point at the wrong machine; an ordinary client is given a dynamic one, so an address is only in use while it is actually needed.

Subnetting divides one network into smaller **subnets** by using some of the host part of the address as a subnet number. It reduces the traffic each part has to carry, because a message for a device in the same subnet need not be passed to the others, and it lets each subnet be managed and secured separately.

△ The two pairs are **independent**. Every address is public *or* private **and** static *or* dynamic – "private" does not mean "dynamic".

2 Practice

Now use the methods above.

2.1 A user enters the URL `https://www.exercises.lol/library/physics.pdf`. State the three parts of this URL and what each one identifies. [3]

2.2 Explain the role of the **Domain Name Service**. [2]

2.3 State the format of an **IPv4** address and the format of an **IPv6** address. [2]

2.4 Explain why **IPv6** was introduced. [2]

2.5 State **one** security implication of a device having a **private** rather than a public IP address. [2]

2.6 State what is meant by a **dynamic** IP address. [1]

3 Exam-style questions

3.1 Which of these is a valid **IPv4** address? [1]

A B
C D

A `192.168.1.300`
B `2001:0db8:85a3::8a2e:0370:7334`
C `192.168.1.20`
D `www.example.com`

3.2 A user types a URL into a web browser and presses enter.

(a) Describe the role of the **Domain Name Service** in what happens next. [3]

(b) Explain why name servers, the operating system and the browser each keep a **cache** of recent DNS results. [2]

(c) State what happens when the name server that is contacted does **not** hold a record for that domain. [2]

3.3 A small company has 40 devices on one network. They reach the internet through a single router.

(a) Explain the difference between a **public** and a **private** IP address, and state which of the two the 40 devices will have. [3]

(b) State **one** security benefit of that arrangement. [2]

(c) Explain the difference between a **static** and a **dynamic** IP address, and give **one** situation in which a static address is necessary. [3]

(d) State what is meant by **subnetting**, and give **one** reason the company might use it. [2]

Solutions

Each answer shows the steps, then the **result**.

2.1

- `https://` is the **protocol**, which identifies the rules used to communicate with the server
- `www.exercises.lol` is the **domain name**, which identifies the **server** holding the resource
- `/library/physics.pdf` is the **path**, which identifies **which resource** on that server

2.2

- DNS holds the mapping from **domain name to IP address**, distributed across many name servers
- so that a browser given a name can obtain the address the data must actually be sent to

2.3

- **IPv4**: **32 bits**, written as four denary numbers in the range 0-255, separated by dots
- **IPv6**: **128 bits**, written as eight groups of four hexadecimal digits, separated by colons

2.4

- IPv4 has only about 4.3 billion addresses (2^{32}), and the number of devices connected to the internet has exhausted them
- IPv6's 128-bit addresses give an address space large enough that running out is not a practical concern

2.5

- a private address is not reachable directly from the internet, because it is unique only inside its own network
- so the device cannot be contacted – or attacked – directly from outside; an attacker must get past the router first

2.6

- an address that is issued to the device when it connects to the network, and which may be a different address the next time it connects

3.1 C

- each part of an IPv4 address must be in the range 0-255, so **A** is invalid
- **B** is an IPv6 address and **D** is a domain name, not an address at all

3.2

(a)

- the browser takes the **domain name** out of the URL and sends it to a **DNS name server**
- the name server looks up the domain name and finds the **IP address** it maps to, asking other name servers if it does not hold the record itself
- the address is returned to the browser, which then sends its request for the resource to that address

(b)

- a cached result answers the next request for the same name immediately, so the page loads faster and no query has to leave the machine
- and it removes an enormous amount of repeated traffic from the name servers, which could not otherwise handle every lookup for every page

(c)

- it passes the query on to another name server, working up the hierarchy – root, then top-level domain, then the **authoritative** server for that domain
- the address found there is returned back down the chain to the browser, and cached along the way

3.3

(a)

- a **public** IP address is unique across the whole internet and can be reached from it
- a **private** IP address is unique only within one network, and a router translates between the private addresses inside and the public address outside
- the 40 devices have **private** addresses; the router holds the single public one

(b)

- none of the 40 devices can be contacted directly from the internet, since their addresses have no meaning outside the company's own network
- so an attacker on the internet cannot reach a device without first getting through the router, which greatly reduces the exposed surface

(c)

- a **static** address is fixed and does not change
- a **dynamic** address is assigned when the device connects, typically by a DHCP server, and may differ next time
- a static address is necessary for anything that must be found at a known address – a web, mail or file **server**, because DNS records point at a fixed address

(d)

- subnetting divides one network into smaller **subnets**, using part of the host portion of the address as a subnet number
- one reason: traffic meant for a device in the same subnet need not be carried by the others, so congestion falls; or each subnet (for example the office and the guest wi-fi)

can be secured and managed separately